WHAT IS CLAIMED IS:

1. A method for conducting surveillance of transmissions over one or more telecommunications networks, the method comprising:

receiving a data packet intended for transmission to a first recipient;

storing the data packet in a buffer;

transmitting the data packet to the first recipient;

determining whether the data packet is flagged for surveillance and, if so, transmitting the data packet to a second recipient; and

releasing the buffer such that another data packet can be stored therein.

2. The method of Claim 1, further comprising, before transmitting the data packet to the first recipient, determining whether the data packet should be flagged for surveillance.

3. The method of Claim 2, wherein determining whether the data packet should be flagged for surveillance comprises determining whether the data packet is being transmitted to or from a telecommunications device associated with an electronic surveillance protocol (ESP) object.

4. The method of Claim 3, wherein the telecommunications device comprises an IP phone.

5. The method of Claim 1, wherein the data packet is received over a hybrid fiber-coax (HFC) network.

6. The method of Claim 1, wherein the data packet is received over a public switched telephone network (PSTN).

7. The method of Claim 1, wherein the data packet comprises a surveillance flag segment, a header segment, and a data segment.

8. The method of Claim 1, wherein the data packet is transmitted to the first recipient over a HFC network.

9. The method of Claim 1, wherein the data packet is transmitted to the first recipient over a PSTN.

10. The method of Claim 1, wherein determining whether the data packet is flagged for surveillance comprises referencing a surveillance flag segment of the data packet.

11. The method of Claim 1, wherein transmitting the data packet to the second recipient comprises transmitting the data packet to a delivery function module (DF).

12. A method for transmitting data packets to a plurality of recipients, the method comprising:

storing a data packet in a buffer, wherein the data packet comprises a header segment having a first destination address;

transmitting the data packet to a recipient at the first destination address;

replacing the first destination address in the header segment of the data packet with a second destination address;

transmitting the data packet to a recipient at the second destination address; and

after transmitting the data packet to the recipient at the second destination address, releasing the buffer such that another data packet can be stored therein.

13. The method of Claim 12, wherein the recipient at the first destination address is the intended recipient of the data packet, and the recipient at the second destination address is a law enforcement official.

14. The method of Claim 12, wherein transmitting the data packet to the recipient at the first destination address comprises transmitting the data packet over a HFC network.

15. The method of Claim 12, wherein transmitting the data packet to the recipient at the first destination address comprises transmitting the data packet over a PSTN.

16. The method of Claim 12, wherein the data packet further comprises a surveillance flag segment and a data segment.

17. A method for creating hash entries in a hash entry table comprising:

receiving an instruction to create a new hash entry in hash entry table stored in a memory of a cable modem termination system (CMTS);

generating a hash entry comprising information about an end-to-end connection between a subscriber using an IP phone and another party;

determining whether transmissions to or from the IP phone are subject to surveillance and, if so, adding surveillance information to the hash entry.

18. The method of Claim 17, wherein the instruction to create a new hash entry is received when a telephone call is initiated with a subscriber using an IP phone.

19. The method of Claim 17, wherein determining whether transmissions to or from the IP phone are subject to surveillance comprises determining whether an ESP object is associated with the IP phone.

20. The method of Claim 17, wherein the surveillance information comprises the destination address of a DF.

21. A CMTS comprising:

a buffer configured to store data packets;

a memory configured to store a hash entry table, wherein the hash entry table includes information regarding whether data packets should be marked for surveillance;

a processor coupled to the buffer and to the memory configured to transmit data packets to their intended recipients,

wherein the processor comprises a surveillance module configured to determine whether a given data packet is marked for surveillance and, if so, transmit the data packet to a surveilling recipient without creating a copy of the data packet.

22. The CMTS of Claim 21, further comprising a cable port in communication with the processor through a cable receiver and a cable transmitter, wherein the cable port is configured to receive transmissions over a HFC network.

23. The CMTS of Claim 21, further comprising a network port in communication with the processor through a network receiver and a network transmitter, wherein the network port is configured to receive transmissions over a PSTN.

24. The CMTS of Claim 21, wherein each data packet comprises a surveillance flag segment, a header segment, and a data segment.

25. The CMTS of Claim 21, wherein the surveillance module is configured to determine whether data packets transmitted to or from an IP phone should be marked for surveillance.

26. The CMTS of Claim 25, wherein the surveillance module determines whether data packets should be marked for surveillance by determining whether an ESP object is associated with the IP phone.

27. The CMTS of Claim 21, wherein the surveillance module determines whether a data packet is marked for surveillance by referencing a surveillance flag segment of the data packet.

28. A data packet comprising:

a data segment containing content to be transmitted from a sender to an intended recipient;

a header segment including address and control information; and

a surveillance flag indicating whether the data packet is marked for surveillance;

wherein, if the surveillance flag indicates that the data packet is marked for surveillance, the data segment of the data packet is transmitted to both the intended recipient and another recipient.

29. A machine readable medium comprising machine readable instructions for causing a computer to perform a method comprising:

receiving a data packet intended for transmission to a first recipient;

storing the data packet in a buffer;

transmitting the data packet to the first recipient;

determining whether the data packet is flagged for surveillance and, if so, transmitting the data packet to a second recipient; and

releasing the buffer such that another data packet can be stored therein.

30. The machine readable medium of Claim 29, wherein the method further comprises, before transmitting the data packet to the first recipient, determining whether the data packet should be flagged for surveillance.

31. The machine readable medium of Claim 30, wherein determining whether the data packet should be flagged for surveillance comprises determining whether the data packet is being transmitted to or from a telecommunications device associated with an ESP object.

32. The machine readable medium of Claim 31, wherein the telecommunications device comprises an IP phone.

33. The machine readable medium of Claim 29, wherein the data packet is received over a HFC network.

34. The machine readable medium of Claim 29, wherein the data packet is received over a PSTN.

35. The machine readable medium of Claim 29, wherein the data packet comprises a surveillance flag segment, a header segment, and a data segment.

36. The machine readable medium of Claim 29, wherein the data packet is transmitted to the first recipient over a HFC network.

37. The machine readable medium of Claim 29, wherein the data packet is transmitted to the first recipient over a PSTN.

38. The machine readable medium of Claim 29, wherein determining whether the data packet is flagged for surveillance comprises referencing a surveillance flag segment of the data packet.

39. The machine readable medium of Claim 29, wherein transmitting the data packet to the second recipient comprises transmitting the data packet to a DF.